Chapitre II
Algorithmes de Chiffrement à Clés Publiques

Protocole Diffie-Hellman

Chiffrement de RSA

Chiffrement de Rabin

Chiffrement de Merkle-Hellman

Chiffrement de ElGamal

PROTOCOLE DE DIFFIE-HELLMAN

- Inventé par Whitfield Diffie et Martin Hellman en 1976

Whitfield Diffie

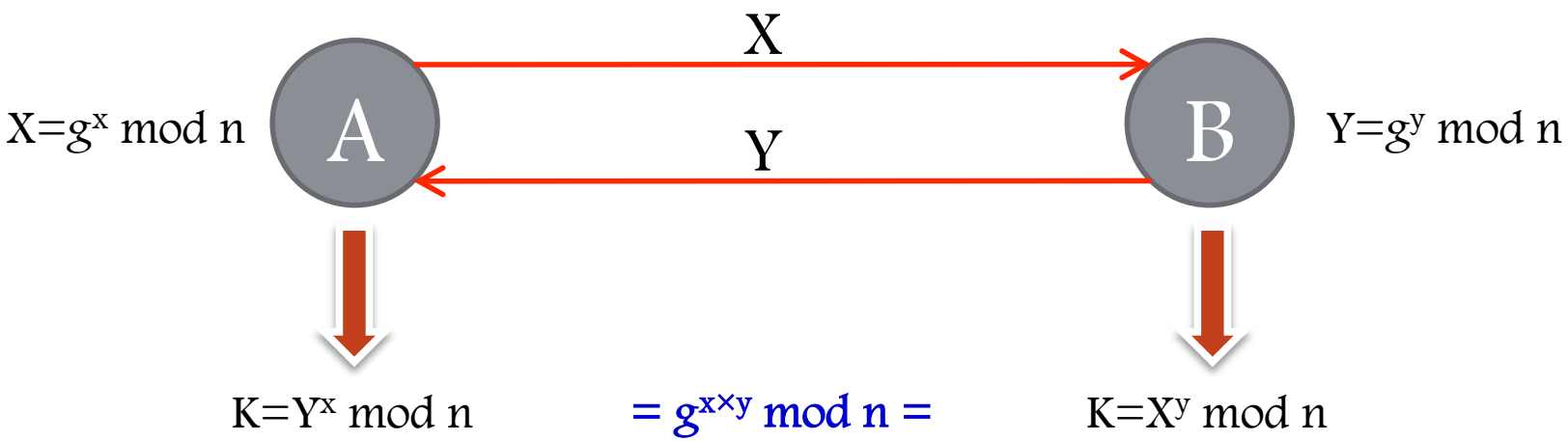
Martin Hellman

- La naissance de la cryptographie à clés asymétriques
- Partage d'une clé secrète par l'intermédiaire d'un échange de données publiques pouvant être interceptées
- Problème du Logarithme Discret ⇒ $A=B^X \bmod C$

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

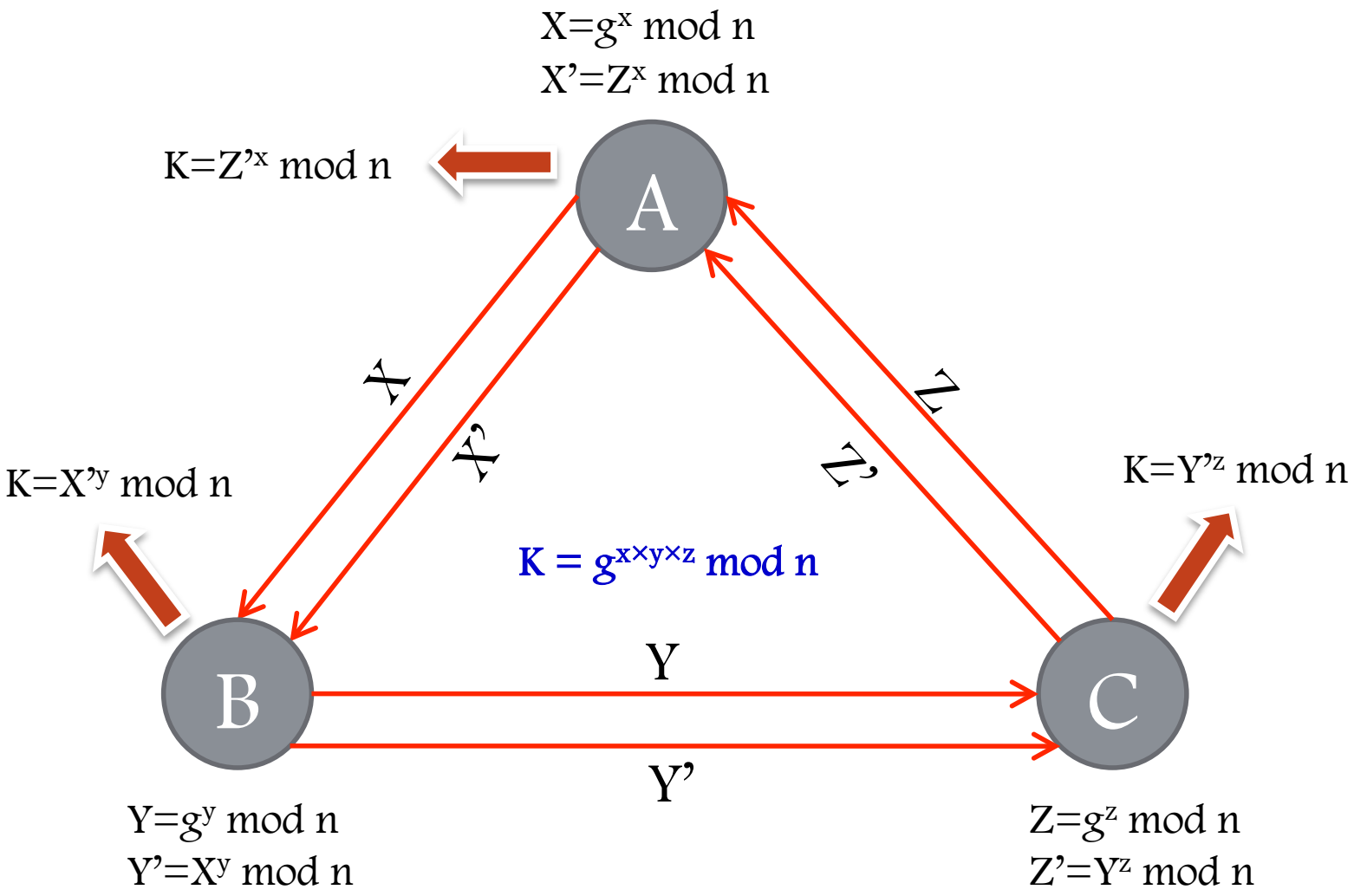
PROTOCOLE DE DIFFIE-HELLMAN

- A et B partagent deux paramètres (g, n) ⇒ publique
- Clé privée de A ⇒ x
- Clé privée de B ⇒ y
- L'intrus intercepte $X=g^x \bmod n$ **?!**



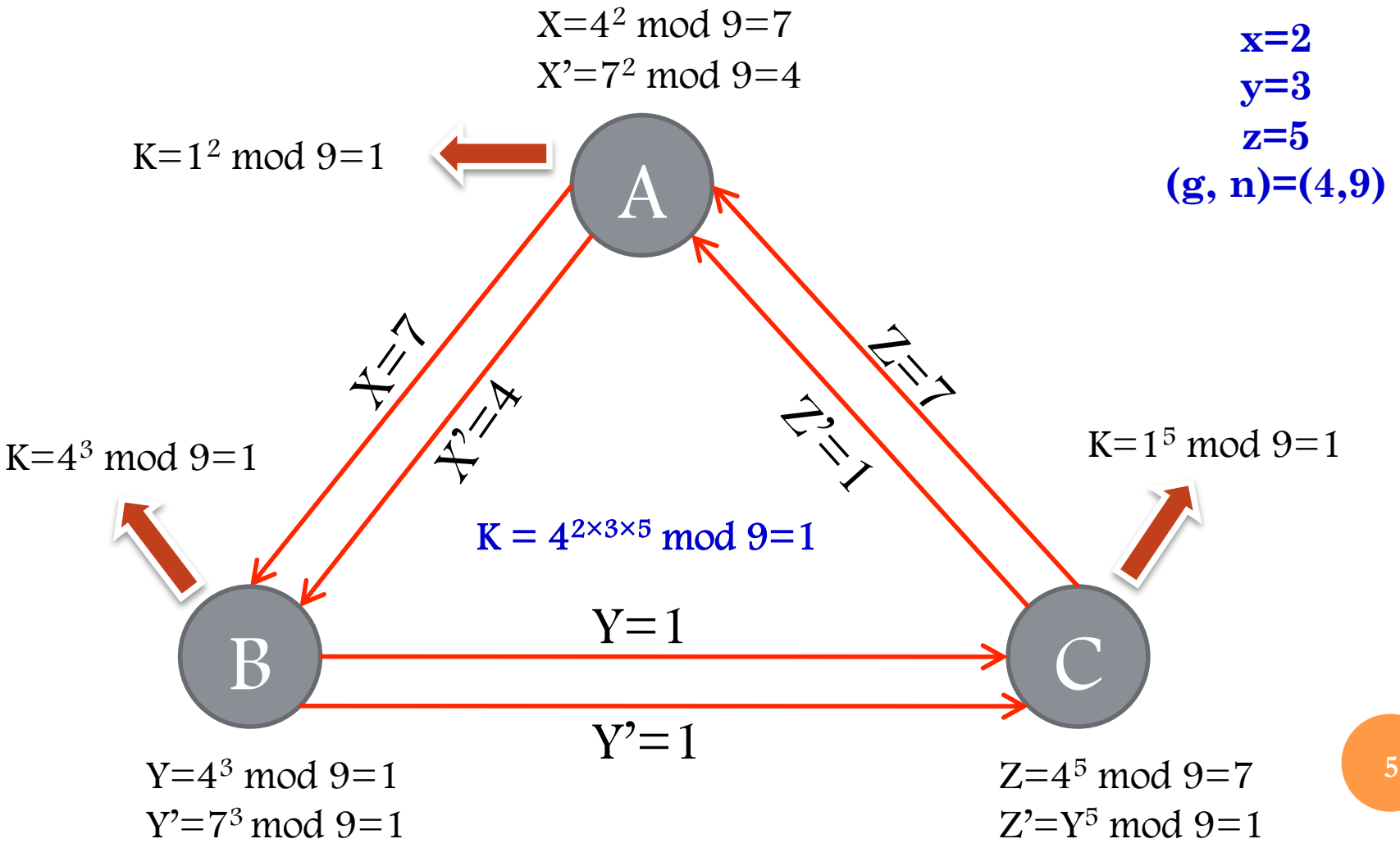
Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

PROTOCOLE DE DIFFIE-HELLMAN



Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

PROTOCOLE DE DIFFIE-HELLMAN

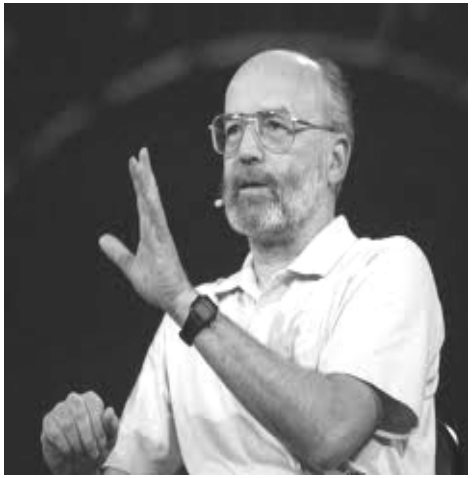


Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

CHIFFREMENT DE RSA

- Inventé par Ron Rivest, Adi Shamir et Leonard Adleman en 1977

Ronald Rivest



Adi Shamir

Leonard Adleman

- Le premier système de chiffrement à clés asymétriques
- Problème de factorisation

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

CHIFFREMENT DE RSA

- Choisir deux grands nombre premiers p et q
- Calculer $n=p\times q$
- Calculer $\phi(n)=(p-1)\times(q-1)$
- Choisir $e < \phi(n)$ tel que $pgcd(e, \phi(n))=1$
- Calculer d tel que $e\times d \bmod \phi(n)=1$
- Clé publique $\Rightarrow$ (e, n)
- Clé privée $\Rightarrow$ (d, n)
- Chiffrement $\Rightarrow C=M^e \bmod n$
- Déchiffrement $\Rightarrow M=C^d \bmod n$

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

CHIFFREMENT DE RABIN

- Inventé par Michael Rabin en 1979

Michael Rabin

- Amélioration du processus de chiffrement
- Problème de factorisation

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

CHIFFREMENT DE RABIN

- Choisir deux nombres premiers p et q :
  - $p \bmod 4 = 3$
  - $q \bmod 4 = 3$
- Clé publique $\Rightarrow n=p\times q$
- Clé privée $\Rightarrow (p, q)$
- Chiffrement $\Rightarrow C=M^2 \bmod n$
- Déchiffrement $\Rightarrow M=C^{1/2} \bmod n$
  - $m_p=C^{(p+1)/4} \bmod p$
  - $m_q=C^{(q+1)/4} \bmod q$
  - $p\times y_p + q\times y_q = 1$
  - $R=(p\times m_q\times y_p + q\times m_p\times y_q) \bmod n$
  - $S=(p\times m_q\times y_p - q\times m_p\times y_q) \bmod n$
  - Solutions possibles : $\{R, S, n-R, n-S\}$

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia